

WHAT IS CLAIMED IS:

1. A method of securely accelerating customer premises equipment based virtual private network transmissions over a carrier network comprising the steps of:

5 establishing an encrypted acceleration tunnel between a VPN acceleration client and a VPN acceleration server in response to a VPN acceleration client request for information;

 transmitting said VPN acceleration client's VPN address and required data information to said VPN acceleration server over said encrypted acceleration tunnel;

10 establishing an encrypted VPN tunnel between said VPN acceleration server and an appropriate VPN switch thus providing access to the appropriate enterprise content servers, said appropriate Enterprise content server corresponding with said required data information transmitted;

 encrypting and transmitting required data corresponding to said required data
15 information from said VPN switch to said VPN acceleration server over said VPN tunnel, said required data is communicated from said appropriate Enterprise content server to said VPN switch prior to encryption and transmission;

 decrypting said required data at said VPN acceleration server;

 accelerating and encrypting by said VPN acceleration server and transmitting
20 said required data to said VPN acceleration client; and

Ref. No. 15377ROUS02U

decrypting said required data in response to said VPN acceleration client receiving said required data.

2. A method as claimed in Claim 1 wherein the step of establishing an encrypted acceleration tunnel uses public key infrastructure (PKI) encryption.

5 3. A method as claimed in Claim 1 wherein the required data information includes at least one of a VPN switch address, user name, and password.

4. A method as claimed in Claim 1 wherein the encrypted VPN tunnel is an IPSec tunnel.

10 5. A method as claimed in Claim 1 wherein the encrypted VPN tunnel is an MPLS tunnel.

6. A method as claimed in Claim 1 wherein the encrypted VPN tunnel is a L2TP tunnel.

7. A server for providing secure virtual private network service for wireless clients comprising:

15 a first module for terminating a virtual private network tunnel to a private network switch;

a second module for accelerating data for transmission over a wireless network; and

a third module for terminating an encrypted tunnel to a wireless client

20 whereby a secure virtual network service is provided between the private network service is provided between the private network and the wireless client, for which acceleration of data on the wireless network is provided.

8. A server as claimed in Claim 7 wherein the virtual private network tunnel is IPSec.

Ref. No. 15377ROUS02U

9. A server as claimed in Claim 7 wherein the virtual private network tunnel is MPLS.
10. A server as claimed in Claim 7 wherein the virtual private network tunnel is L2TP.
- 5 11. A server as claimed in Claim 7 wherein the encrypted tunnel is public key infrastructure encrypted.